(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－331449
（P2001－331449A）
(43)公開日　平成13年11月30日(2001.11.30)

| (51)Int.Cl.⁷ | | 識別記号 | FI | | テーマコード(参考) |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 15/00 | ３３０ | Ｇ０６Ｆ | 15/00 | ３３０Ｂ |
| | 12/14 | ３２０ | | 12/14 | ３２０Ａ |
| Ｈ０４Ｌ | 9/32 | | Ｈ０４Ｌ | 9/00 | ６７３Ｃ |
| | | | | | ６７５Ａ |

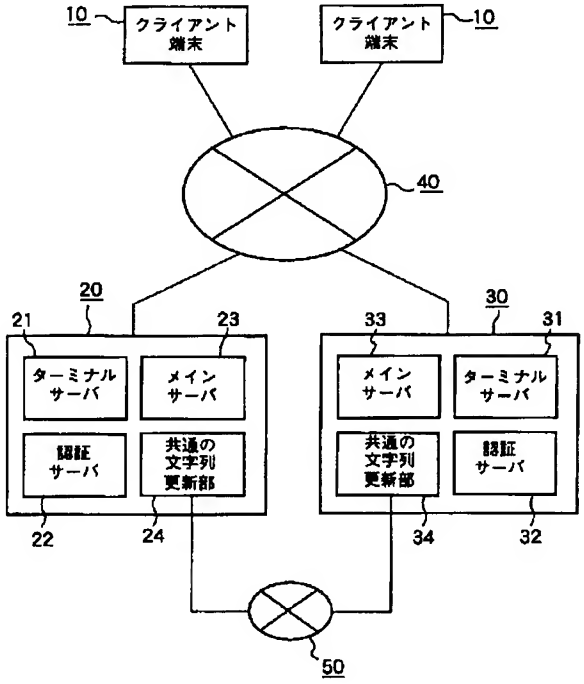
審査請求　有　　請求項の数20　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－61999(P2001－61999)
(22)出願日　平成13年３月６日(2001.3.6)
(31)優先権主張番号　特願2000－69079(P2000－69079)
(32)優先日　平成12年３月13日(2000.3.13)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　500257300
ヤフー株式会社
東京都港区北青山３－６－７
(72)発明者　楠　正憲
東京都世田谷区千歳台１－21－１　ジェー・ステージ千歳台101号室
(74)代理人　100058479
弁理士　鈴江　武彦　（外５名）

(54)【発明の名称】　アクセス認証システム、記憶媒体、プログラム及びアクセス認証方法

(57)【要約】
【課題】１つのサーバに対しての個人情報に基づいて、各種サービスを提供する他のサーバを利用可能とするアクセス認証システムを提供すること。
【解決手段】クライアント端末１０から入力された個別情報に基づいて第１のターミナルサーバへの接続の可否を認証するとともに、クライアントパラメータＰを符号化した第１のチケットデータを作成し、第２のターミナルサーバに転送する第１の認証サーバ２２と、クライアントパラメータＰの正当性及び第１のチケットデータＤ１の行使の有無を検証するとともに、クライアントパラメータＰを符号化した第２のチケットデータＤ２を作成し、第２のチケットデータＤ２と第１のチケットデータＤ１とを照合し、第２のターミナルサーバ３１へクライアント端末１０の接続可否を指示する第２の認証サーバ３２とを備えている。



1

【特許請求の範囲】

【請求項１】第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第１のターミナルサーバに対して上記クライアントから入力された個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成し、上記第２のターミナルサーバに転送する第１の認証サーバと、

上記クライアントパラメータの正当性及び上記第１のチケットデータの行使の有無を検証するとともに、上記クライアントパラメータを所定の規則で符号化した第２のチケットデータを作成し、この第２のチケットデータと上記第１のチケットデータとを照合し、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証サーバとを備えていることを特徴とするアクセス認証システム。

【請求項２】上記所定の規則は、一方向関数による要約であることを特徴とする請求項１に記載のアクセス認証システム。

【請求項３】上記クライアントパラメータには、上記クライアントのＩＤ、アクセス元ＩＰアドレス、上記第１のチケットデータの有効期限のうち少なくとも１つが含められていることを特徴とする請求項１に記載のアクセス認証システム。

【請求項４】上記第１及び第２の認証サーバにおいて、上記第１及び第２のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする請求項１に記載のアクセス認証システム。

【請求項５】上記共通の文字列は、所定のタイミングで変更されるものであることを特徴とする請求項４に記載のアクセス認証システム。

【請求項６】第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第１のターミナルサーバに対して上記クライアントから入力されたＩＤ及びパスワードに基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記ＩＤ、上記クライアントのアクセス元ＩＰアドレス、所定の有効期限、共通の文字列からなるクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成し、上記第２のターミナルサーバに転送する第１の認証サーバと、

上記第２のターミナルサーバに対して上記クライアントから入力されたアクセス元ＩＰアドレスと上記クライアントパラメータのアクセス元ＩＰアドレスとを照合し、上記有効期限内のアクセスであるか否かを判断し、上記第１のチケットデータの行使の有無を判断し、上記クライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成し、この第２のチケットデータと上記第１のチケットデータとを照合することで、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証サーバとを備えていることを特徴とするアクセス認証システム。

2

【請求項７】第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第１のターミナルサーバにおいて上記クライアントから入力された個別情報を取得する第１の個別情報取得手段と、

上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証する第１の認証手段と、

上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成する第１のチケットデータ作成手段と、

上記第２のターミナルサーバに転送する転送手段と、

上記第２のターミナルサーバにおいて上記クライアントから入力された個別情報を取得する第２の個別情報取得手段と、

上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第２のチケットデータを作成し、この第２のチケットデータと上記第１のチケットデータとを照合し、上記第２のターミナルサーバへ上記クライアントの接続可否を認証する第２の認証手段とを備えていることを特徴とするアクセス認証システム。

【請求項８】上記所定の規則は、一方向関数による要約であることを特徴とする請求項７に記載のアクセス認証システム。

【請求項９】上記第１及び第２のチケットデータ作成手段は、上記第１及び第２のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする請求項７に記載のアクセス認証システム。

【請求項１０】上記第２の認証手段は、上記第１のチケットデータの有効性を判断することを特徴とする請求項７に記載のアクセス認証システム。

【請求項１１】上記第２の認証手段は、上記クライアントパラメータの正当性を判断することを含むことを特徴とする請求項７に記載のアクセス認証システム。

【請求項１２】第１のターミナルサーバを経由してクライアントに接続サービスを行うアクセス認証システムにおいて、

上記クライアントから個別情報を取得する第１の個別情報取得手段と、

上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証する第１認証手段と、

この第１認証手段にて認証が可とされた場合に、少なく

とも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成する第１のチケットデータ作成手段と、
上記第１のチケットデータを転送する転送手段とを備えていることを特徴とするアクセス認証システム。
【請求項１３】クライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、
上記クライアントの個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを取得する第１のチケットデータ取得手段と、
上記クライアントから個別情報を取得する第２の個別情報取得手段と、
この第２の個別情報取得手段にて取得された個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成する第２のチケットデータ作成手段と、
上記第２のチケットデータと上記第１のチケットデータとを照合し、上記第２のターミナルサーバへ上記クライアントの接続可否を判断する判断手段とを備えていることを特徴とするアクセス認証システム。
【請求項１４】コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、
第１のターミナルサーバにおいてクライアントから個別情報を取得させる第１の個別情報取得手段と、
上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証させる第１認証手段と、
上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成させる第１のチケットデータ作成手段と、
上記第１のチケットデータを第２のターミナルサーバに転送させる転送手段と、
上記第２のターミナルサーバにおいて上記第１のチケットデータを取得させる第１のチケットデータ取得手段と、
上記第２のターミナルサーバにおいて上記クライアントから個別情報を取得させる第２の個別情報取得手段と、
上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成させる第２のチケットデータ作成手段と、
上記第１のチケットデータと上記第２のチケットデータとを照合し、上記第２のターミナルサーバへの上記クライアントの接続可否を認証させる第２認証手段とを備えていることを特徴とする記憶媒体。
【請求項１５】コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、
第１のターミナルサーバにおいてクライアントから個別情報を取得させる第１の個別情報取得手段と、
上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証させる第１認証手段と、
上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成させる第１のチケットデータ作成手段と、
上記第１のチケットデータを転送させる転送手段とを備えていることを特徴とする記憶媒体。
【請求項１６】コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、
第２のターミナルサーバにおいて上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した上記第１のチケットデータを取得させる第１のチケットデータ取得手段と、
上記第２のターミナルサーバにおいて上記クライアントから個別情報を取得させる第２の個別情報取得手段と、
上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成させる第２のチケットデータ作成手段と、
上記第１のチケットデータと上記第２のチケットデータとを照合し、上記第２のターミナルサーバへの上記クライアントの接続可否を認証させる第２認証手段とを備えていることを特徴とする記憶媒体。
【請求項１７】コンピュータを動作させるためのプログラムにおいて、
第１のターミナルサーバにおいてクライアントから個別情報を取得させる第１の個別情報取得手段と、
上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証させる第１認証手段と、
上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成させる第１のチケットデータ作成手段と、
上記第１のチケットデータを第２のターミナルサーバに転送させる転送手段と、
上記第２のターミナルサーバにおいて上記第１のチケットデータを取得させる第１のチケットデータ取得手段と、
上記第２のターミナルサーバにおいて上記クライアントから個別情報を取得させる第２の個別情報取得手段と、
上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成させる第２のチケットデータ作成手段と、
上記第１のチケットデータと上記第２のチケットデータとを照合し、上記第２のターミナルサーバへの上記クラ

イアントの接続可否を認証させる第２認証手段とを備えていることを特徴とするプログラム。

【請求項１８】コンピュータを動作させるためのプログラムにおいて、

第１のターミナルサーバにおいてクライアントから個別情報を取得させる第１の個別情報取得手段と、

上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証させる第１認証手段と、

上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成させる第１のチケットデータ作成手段と、

上記第１のチケットデータを転送させる転送手段とを備えていることを特徴とするプログラム。

【請求項１９】コンピュータを動作させるためのプログラムにおいて、

第２のターミナルサーバにおいてクライアントの個別情報の一部を含むクライアントパラメータを所定の規則で符号化した上記第１のチケットデータを取得させる第１のチケットデータ取得手段と、

上記第２のターミナルサーバにおいて上記クライアントから個別情報を取得させる第２の個別情報取得手段と、

上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成させる第２のチケットデータ作成手段と、

上記第１のチケットデータと上記第２のチケットデータとを照合し、上記第２のターミナルサーバへの上記クライアントの接続可否を認証させる第２認証手段とを備えていることを特徴とするプログラム。

【請求項２０】第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証方法において、

上記第１のターミナルサーバへの上記クライアントの接続の可否を認証する第１の認証ステップと、

上記クライアントから入力された個別情報の少なくとも一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成する第１チケットデータ作成ステップと、

上記第２のターミナルサーバに上記クライアントパラメータ及び上記第１のチケットデータを転送するデータ転送ステップと、

上記第１のターミナルサーバにおける上記クライアントパラメータの正当性及び上記第１のチケットデータの行使の有無を検証する検証ステップと、

上記クライアントパラメータを所定の規則で符号化した第２のチケットデータを作成する第２チケットデータ作成ステップと、

この第２のチケットデータと上記第１のチケットデータとを照合するチケットデータ照合ステップと、



上記検証ステップ及び上記チケットデータ照合ステップにおける結果に基づいて、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証ステップとを備えていることを特徴とするアクセス認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、所定のアプリケーションプロバイダへのアクセス権を予め有するユーザが異なるアプリケーションプロバイダへのアクセス権を得るためのアクセス認証システム及びアクセス認証方法に関する。

【０００２】

【従来の技術】ユーザはインターネットを介して様々な情報サービス等の各種サービスを提供するサービス提供者を利用することができる。サービス提供者とは、インターネットを介して接続されたクライアント端末に対してデータやコンテンツを提供したり、情報処理サービスを提供する業者を指している。サービス提供者はそれぞれ独立しており、ユーザは利用したいサービス提供者と契約し、それぞれＩＤとパスワードを持つことでアクセス権を得るようにしている。

【０００３】

【発明が解決しようとする課題】しかし、サービス提供者は増えており、ユーザがそれぞれのサービス提供者と契約するのはＩＤやパスワードを管理する上で煩雑であった。また、各サービス提供者が提供できるサービスの種類には限界があった。

【０００４】一方、一つのＩＤとパスワードを複数のサービス提供者間で共通化して用いる方法も考えられるが、ＩＤ及びパスワードの両方を各サービス提供者で保持することになるため、課金や秘密保持の点で問題があった。

【０００５】そこで本発明は、１つのサーバ（サービス提供者）に対しての個人情報（ＩＤ及びパスワード）のみで、各種サービスを提供する他のサーバ（サービス提供者）を個人情報の全てを開示することなく利用することができるようにするためのアクセス認証システム、記憶媒体、プログラム及びアクセス認証方法を提供することを目的としている。

【０００６】

【課題を解決するための手段】上記課題を解決し目的を達成するために、本発明のアクセス認証システム、記憶媒体、プログラム及びアクセス認証方法は次のように構成されている。

【０００７】（１）第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、上記第１のターミナルサーバに対して上記クライアントから入力された個別情報に基づいて上記第１のターミナルサーバへの

上記クライアントの接続の可否を認証するとともに、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成し、上記第２のターミナルサーバに転送する第１の認証サーバと、上記クライアントパラメータの正当性及び上記第１のチケットデータの行使の有無を検証するとともに、上記クライアントパラメータを所定の規則で符号化した第２のチケットデータを作成し、この第２のチケットデータと上記第１のチケットデータとを照合し、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証サーバとを備えていることを特徴とする。

【０００８】（２）上記（１）に記載されたアクセス認証システムであって、上記所定の規則は、一方向関数による要約であることを特徴とする。

【０００９】（３）上記（１）に記載されたアクセス認証システムであって、上記クライアントパラメータには、上記クライアントのＩＤ、アクセス元ＩＰアドレス、上記第１のチケットデータの有効期限のうち少なくとも１つが含められていることを特徴とする。

【００１０】（４）上記（１）に記載されたアクセス認証システムであって、上記第１及び第２の認証サーバにおいて、上記第１及び第２のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする。

【００１１】（５）上記（４）に記載されたアクセス認証システムであって、上記共通の文字列は、所定のタイミングで変更されるものであることを特徴とする。

【００１２】（６）第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、上記第１のターミナルサーバに対して上記クライアントから入力されたＩＤ及びパスワードに基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記ＩＤ、上記クライアントのアクセス元ＩＰアドレス、所定の有効期限、共通の文字列からなるクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成し、上記第２のターミナルサーバに転送する第１の認証サーバと、上記第２のターミナルサーバに対して上記クライアントから入力されたアクセス元ＩＰアドレスと上記クライアントパラメータのアクセス元ＩＰアドレスとを照合し、上記有効期限内のアクセスであるか否かを判断し、上記第１のチケットデータの行使の有無を判断し、上記クライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成し、この第２のチケットデータと上記第１のチケットデータとを照合することで、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証サーバとを備えていることを特徴とする。

【００１３】（７）第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、上記第１のターミナルサーバにおいて上記クライアントから入力された個別情報を取得する第１の個別情報取得手段と、上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証する第１の認証手段と、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成する第１のチケットデータ作成手段と、上記第２のターミナルサーバに転送する転送手段と、上記第２のターミナルサーバにおいて上記クライアントから入力された個別情報を取得する第２の個別情報取得手段と、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第２のチケットデータを作成し、この第２のチケットデータと上記第１のチケットデータとを照合し、上記第２のターミナルサーバへ上記クライアントの接続可否を認証する第２の認証手段とを備えていることを特徴とする。

【００１４】（８）上記（７）に記載されたアクセス認証システムであって、上記所定の規則は、一方向関数による要約であることを特徴とする。

【００１５】（９）上記（７）に記載されたアクセス認証システムであって、上記第１及び第２のチケットデータ作成手段は、上記第１及び第２のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする。

【００１６】（１０）上記（７）に記載されたアクセス認証システムであって、上記第２の認証手段は、上記第１のチケットデータの有効性を判断することを特徴とする。

【００１７】（１１）上記（７）に記載されたアクセス認証システムであって、上記第２の認証手段は、上記クライアントパラメータの正当性を判断することを含むことを特徴とする。

【００１８】（１２）第１のターミナルサーバを経由してクライアントに接続サービスを行うアクセス認証システムにおいて、上記クライアントから個別情報を取得する第１の個別情報取得手段と、上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証する第１認証手段と、この第１認証手段にて認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成する第１のチケットデータ作成手段と、上記第１のチケットデータを転送する転送手段とを備えていることを特徴とする。

【００１９】（１３）クライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、上記クライアントの個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを取得する第１のチケットデータ取得手段

と、上記クライアントから個別情報を取得する第２の個別情報取得手段と、この第２の個別情報取得手段にて取得された個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成する第２のチケットデータ作成手段と、上記第２のチケットデータと上記第１のチケットデータとを照合し、上記第２のターミナルサーバへ上記クライアントの接続可否を判断する判断手段とを備えていることを特徴とする。

【００２０】（１４）コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、第１のターミナルサーバにおいてクライアントから個別情報を取得させる第１の個別情報取得手段と、上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証させる第１認証手段と、上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成させる第１のチケットデータ作成手段と、上記第１のチケットデータを第２のターミナルサーバに転送させる転送手段と、上記第２のターミナルサーバにおいて上記第１のチケットデータを取得させる第１のチケットデータ取得手段と、上記第２のターミナルサーバにおいて上記クライアントから個別情報を取得させる第２の個別情報取得手段と、上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成させる第２のチケットデータ作成手段と、上記第１のチケットデータと上記第２のチケットデータとを照合し、上記第２のターミナルサーバへの上記クライアントの接続可否を認証させる第２認証手段とを備えていることを特徴とする。

【００２１】（１５）コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、第１のターミナルサーバにおいてクライアントから個別情報を取得させる第１の個別情報取得手段と、上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証させる第１認証手段と、上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成させる第１のチケットデータ作成手段と、上記第１のチケットデータを転送させる転送手段とを備えていることを特徴とする。

【００２２】（１６）コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、第２のターミナルサーバにおいて上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した上記第１のチケットデータを取得させる第１のチケットデータ取得手段と、上記第２のターミナルサーバにおいて上記クライアントから個別情報を取得させる第２の個別情報取得手段と、上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成させる第２のチケットデータ作成手段と、上記第１のチケットデータと上記第２のチケットデータとを照合し、上記第２のターミナルサーバへの上記クライアントの接続可否を認証させる第２認証手段とを備えていることを特徴とする。

【００２３】（１７）コンピュータを動作させるためのプログラムにおいて、第１のターミナルサーバにおいてクライアントから個別情報を取得させる第１の個別情報取得手段と、上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証させる第１認証手段と、上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成させる第１のチケットデータ作成手段と、上記第１のチケットデータを第２のターミナルサーバに転送させる転送手段と、上記第２のターミナルサーバにおいて上記第１のチケットデータを取得させる第１のチケットデータ取得手段と、上記第２のターミナルサーバにおいて上記クライアントから個別情報を取得させる第２の個別情報取得手段と、上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成させる第２のチケットデータ作成手段と、上記第１のチケットデータと上記第２のチケットデータとを照合し、上記第２のターミナルサーバへの上記クライアントの接続可否を認証させる第２認証手段とを備えていることを特徴とする。

【００２４】（１８）コンピュータを動作させるためのプログラムにおいて、第１のターミナルサーバにおいてクライアントから個別情報を取得させる第１の個別情報取得手段と、上記個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証させる第１認証手段と、上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成させる第１のチケットデータ作成手段と、上記第１のチケットデータを転送させる転送手段とを備えていることを特徴とする。

【００２５】（１９）コンピュータを動作させるためのプログラムにおいて、第２のターミナルサーバにおいてクライアントの個別情報の一部を含むクライアントパラメータを所定の規則で符号化した上記第１のチケットデータを取得させる第１のチケットデータ取得手段と、上記第２のターミナルサーバにおいて上記クライアントから個別情報を取得させる第２の個別情報取得手段と、上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成さ

せる第２のチケットデータ作成手段と、上記第１のチケットデータと上記第２のチケットデータとを照合し、上記第２のターミナルサーバへの上記クライアントの接続可否を認証させる第２認証手段とを備えていることを特徴とする。

【００２６】（２０）第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証方法において、上記第１のターミナルサーバへの上記クライアントの接続の可否を認証する第１の認証ステップと、上記クライアントから入力された個別情報の少なくとも一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成する第１チケットデータ作成ステップと、上記第２のターミナルサーバに上記クライアントパラメータ及び上記第１のチケットデータを転送するデータ転送ステップと、上記第１のターミナルサーバにおける上記クライアントパラメータの正当性及び上記第１のチケットデータの行使の有無を検証する検証ステップと、上記クライアントパラメータを所定の規則で符号化した第２のチケットデータを作成する第２チケットデータ作成ステップと、この第２のチケットデータと上記第１のチケットデータとを照合するチケットデータ照合ステップと、上記検証ステップ及び上記チケットデータ照合ステップにおける結果に基づいて、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証ステップとを備えていることを特徴とする。

【００２７】

【発明の実施の形態】図１は本発明の一実施の形態に係るアクセス認証システムの構成を示す図、図２の（ａ），（ｂ）は同アクセス認証システムに組み込まれた認証サーバ２２，３２の構成を示すブロック図、図３はアクセス認証の手順を示すフロー図である。なお、本実施の形態はソフトウエア処理により実現する場合も含まれる。

【００２８】図１中１０はユーザのクライアント端末、２０はユーザと契約関係にあるサービス提供先サービス提供者、３０はユーザと直接の契約関係にないサービス提供元サービス提供者、４０はインターネット回線、５０は電話回線を示している。

【００２９】サービス提供先サービス提供者２０は、インターネット回線４０に接続されたターミナルサーバ（第１のターミナルサーバ）２１と、このターミナルサーバ２１に接続され後述するような認証等を行う認証サーバ（第１の認証サーバ）２２と、ターミナルサーバ２２に接続されるとともに情報サービスを提供するメインサーバ２３と、電話回線５０に接続された共通の文字列更新部２４とを備えている。

【００３０】認証サーバ２２は、第１のターミナルサーバ２１に対してクライアント端末１０から入力されたＩＤ及びパスワードに基づいてターミナルサーバ２１へのクライアント端末１０からの接続の可否を認証する認証部２２ａと、クライアント端末１０のアクセス元ＩＰアドレスを検出するＩＰアドレス検出部２２ｂと、後述する第１チケット（第１のチケットデータ）の有効期限を生成する有効期限生成部２２ｃと、クライアントパラメータＰ、すなわちＩＤ、クライアントのアクセス元ＩＰアドレス、有効期限生成部２２ｃで生成された有効期限、共通の文字列更新部２４で更新された最新の共通の文字列を一方向関数で要約する等の所定の規則を用いて第１チケットデータＤ１を作成するチケットデータ生成部２２ｄと、クライアントパラメータＰ及び第１チケットデータを認証サーバ３２にインターネット回線４０及びターミナルサーバ３１を介して転送する転送部２２ｅとを備えている。

【００３１】サービス提供元サービス提供者３０は、インターネット回線４０に接続されたターミナルサーバ（第２のターミナルサーバ）３１と、このターミナルサーバ３１に接続され後述するような認証等を行う認証サーバ（第２の認証サーバ）３２と、ターミナルサーバ３１に接続されるとともに情報サービスを提供するメインサーバ３３と、電話回線５０に接続された共通の文字列更新部３４とを備えている。

【００３２】認証サーバ３２は、ターミナルサーバ３１に対してクライアント端末１０から入力されたアクセス元ＩＰアドレスと上述した認証サーバ２２から転送されたクライアントパラメータＰのアクセス元ＩＰアドレスとを照合するアクセス元ＩＰアドレス照合部３２ａと、有効期限内のアクセスであるか否かを判断する有効期限判断部３２ｂと、第１のチケットデータＤ１の行使の有無を判断するチケット行使判断部３２ｃと、転送されたクライアントパラメータＰを上述した規則と同一の規則で符号化した第２のチケットデータＤ２を作成するチケットデータ生成部３２ｄと、第２のチケットデータＤ２と第１のチケットデータＤ１とを照合することで、第２のターミナルサーバ３１へクライアント端末１０からの接続可否を指示する認証部３２ｅとを備えている。

【００３３】共通の文字列更新部２４及び共通の文字列更新部３４は、文字列から構成される同一の共通の文字列を保持しており、定期的に更新されている。

【００３４】このように構成されていると、ユーザがクライアント端末１０からメインサーバ３３にアクセスする場合には次のように行われる。すなわち、ユーザはクライアント端末１０からインターネット回線４０を介してターミナルサーバ２１に接続を行う。このとき、ユーザはサービス提供先サービス提供者が提供するログイン画面に自己のＩＤ及びパスワードを入力する（ＳＴ１０）。このとき、ターミナルサーバ２１では、任意のアクセス制限を行い（ＳＴ１１）、アクセスが禁止された場合にはログインが拒否される（ＳＴ１２）。

【００３５】ＳＴ２においてアクセスが許可された場合

には、ＩＤ、パスワード、アクセス元ＩＰアドレスが認証サーバ２２に送られ、認証部２２ａにてＩＤ及びパスワードに基づいてユーザ認証を行い（ＳＴ１３）、認証に失敗した場合にはログインが拒否される（ＳＴ１４）。なお、この時点でメインサーバ２３へのアクセスが許可される。

【００３６】ＳＴ４においてユーザ認証が成功した場合には、ＩＰアドレス検出部２２ｂにおいてクライアント端末１０のアクセス元ＩＰアドレスが検出され、有効期限生成部２２ｃにおいて第１チケットデータＤ１の有効期限を生成する。そして、チケットデータ生成部２２ｄにおいて、クライアントパラメータＰ（ＩＤ、アクセス元ＩＰアドレス、有効期限、共通の文字列）を一方向関数で要約して第１チケットデータＤ１を作成する（ＳＴ１５）。

【００３７】次に、転送部２２ｅによりクライアントパラメータＰ及び第１チケットデータＤ１を認証サーバ３２にインターネット回線４０及びターミナルサーバ３１を介して転送する（ＳＴ１６）。

【００３８】サービス提供元サービス提供者３０の認証サーバ３２では、アクセス元ＩＰアドレス照合部３２ａによりアクセス元ＩＰアドレス照合部３２ａターミナルサーバ３１に対してクライアント端末１０から入力されたアクセス元ＩＰアドレスと上述した認証サーバ２２から転送されたクライアントパラメータＰのアクセス元ＩＰアドレスとを照合し（ＳＴ２０）、不一致である場合にはログインは拒否される（ＳＴ２１）。

【００３９】次に、有効期限判断部３２ｂにより、有効期限内のアクセスであるか否かを判断し（ＳＴ２２）、有効期限を経過している場合には無効とされログインは拒否される（ＳＴ２３）。

【００４０】次に、チケット行使判断部３２ｃにより、第１のチケットデータＤ１の行使の有無を判断し（ＳＴ２４）、既に行使されている場合にはログインは拒否される（ＳＴ２５）。

【００４１】次に、チケットデータ生成部３２ｄにより、転送されたクライアントパラメータＰを上述した一方向関数で要約した第２のチケットデータＤ２を作成し、第１のチケットデータＤ１とを照合し（ＳＴ２６）、不一致の場合にはログインは拒否される（ＳＴ２７）。

【００４２】次に、ＩＤが既に登録されているものか否かを検索し（ＳＴ２８）、登録されていれば後述するＳＴ３０に進み、登録されていなければＩＤが作成される（ＳＴ２９）。そして、メインサーバ３３へのログインが可能となる（ＳＴ３０）。

【００４３】なお、このようなアクセス認証システムの場合には、サービス提供先サービス提供者２０からサービス提供元サービス提供者３０にクライアントパラメータＰが転送される際に、何らかの方法でクライアントパラメータＰを傍受し、クライアントパラメータＰを改竄して不正アクセスしようとしても、第１のチケットデータＤ１と改竄されたクライアントパラメータＰに基づいて作成された第２のチケットデータＤ２とが不一致となり、ログインが拒否されることになる。

【００４４】なお、改竄されたクライアントパラメータＰに基づいて第１のチケットデータＤ１を作ることにより、新たなサービス提供元サービス提供者３０へのログインが可能になる。しかしながら、第１のチケットデータＤ１の作成には共通の文字列を知る必要がある。しかも、この共通の文字列は、認証サーバ２２，３２に侵入して入手したり、総当たり法によって推測したり、一方向関数の逆演算して導き出すことが考えられるが、共通の文字列の更新を十分に短く設定することで、事実上共通の文字列を入手することが困難になる。

【００４５】また、クライアントパラメータＰ及び第１のチケットデータＤ１を流用しようとしても、有効期限を十分に短く設定しておけば、有効期限後のアクセスとなる可能性が高く、ログインが拒否されることになる。

【００４６】さらに、有効期限内の使用であっても、正規のユーザによるサービス提供元サービス提供者３０へのアクセスは、サービス提供先サービス提供者２０へのアクセスとほぼ同時である。このため、クライアントパラメータＰ及び第１のチケットデータＤ１を第三者が傍受し不正使用しようとしても、既に正規のユーザによって第１のチケットデータＤ１の行使が済んでおり、第三者の第１のチケットデータＤ１ではログインができない。

【００４７】一方、正規なユーザが共通の文字列を含んだ状態で生成された第１のチケットデータＤ１をサービス提供元サービス提供者３０に到達した時点で、共通の文字列が更新されていて第２のチケットデータＤ２と第１のチケットデータＤ１が異なってしまいログインが拒絶されてしまう問題は、次のようにして解決する。

【００４８】例えば、定期的にＡ，Ｂ，Ｃ，Ｄという順番で共通の文字列を変える場合、ＡＢ，ＢＣ，ＣＤ，…というように２つの共通の文字列を組み合わせることで、２種類の第１のチケットデータＤ１を作成し、この２つの第１のチケットデータＤ１のいずれかが第２のチケットデータＤ２と一致すればログイン可能とするように設定することにより対処する。

【００４９】上述したように、本発明の一実施の形態に係るアクセス認証システムによれば、クライアントは、１つのサービス提供先サービス提供者に対してのＩＤ及びパスワードのみで、各種サービスを提供する他のサービス提供元サービス提供者にパスワードを開示することなく利用することが可能となる。また、サービス提供先サービス提供者からサービス提供元サービス提供者に転送されるデータが第三者により傍受された場合であっても、何重にも安全対策が講じられているため、サービス

15

提供元サービス提供者に不正にアクセスがされることがない。

【００５０】なお、上述したシステムは、各サーバ等のコンピュータにインストールされたプログラムの指示に基づき実行されるものであってもよく、また、プログラムの指示に基づきコンピュータ上で稼動しているオペレーティングシステム、ミドルウエア等が各処理の一部を実行するようにしてもよい。

【００５１】また、プログラムは、コンピュータが読取可能な記憶媒体に格納された状態で提供されるようにしてもよい。例えば、記憶媒体としては、磁気ディスク、フロッピー（登録商標）ディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ等）、ＭＯ、半導体メモリ等のようにプログラムを記憶でき、コンピュータが読取可能であるようなものであればよい。

【００５２】さらに、プログラムは、ＬＡＮやインターネット等により伝送されるようにしたものでもよい。

【００５３】なお、本発明は前記実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲で種々変形実施可能であるのは勿論である。

16

＊【００５４】

【発明の効果】本発明によれば、クライアントは、１つのサーバ（サービス提供者）に対しての個人情報（ＩＤ及びパスワード）のみで、各種サービスを提供する他のサーバ（サービス提供者）を個人情報の全てを開示することなく利用することが可能となる。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係るアクセス認証システムの構成を示す図。

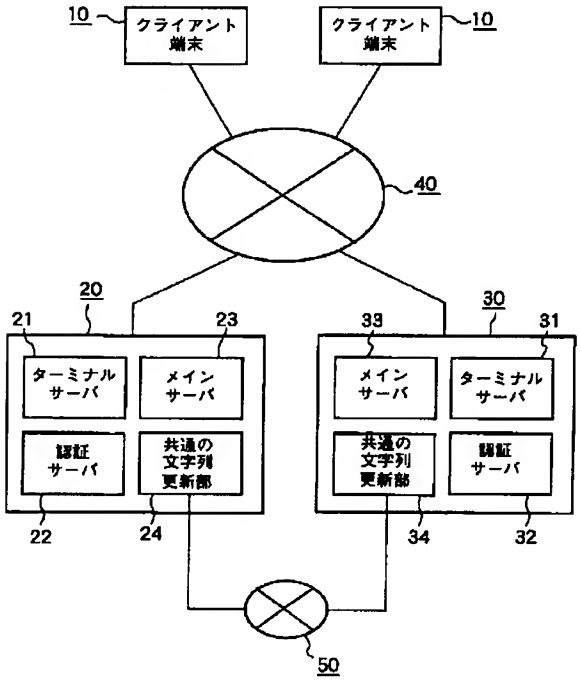
【図２】同アクセス認証システムに組み込まれた認証サーバの構成を示すブロック図。

【図３】同アクセス認証システムの動作を示すフロー図。

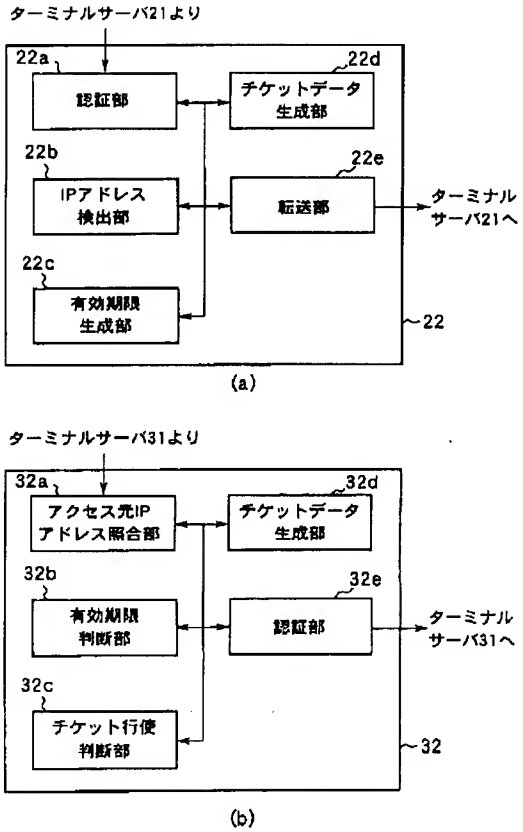
【符号の説明】

１０…クライアント端末
２０…サービス提供先サービス提供者
３０…サービス提供元サービス提供者
４０…インターネット回線
５０…電話回線

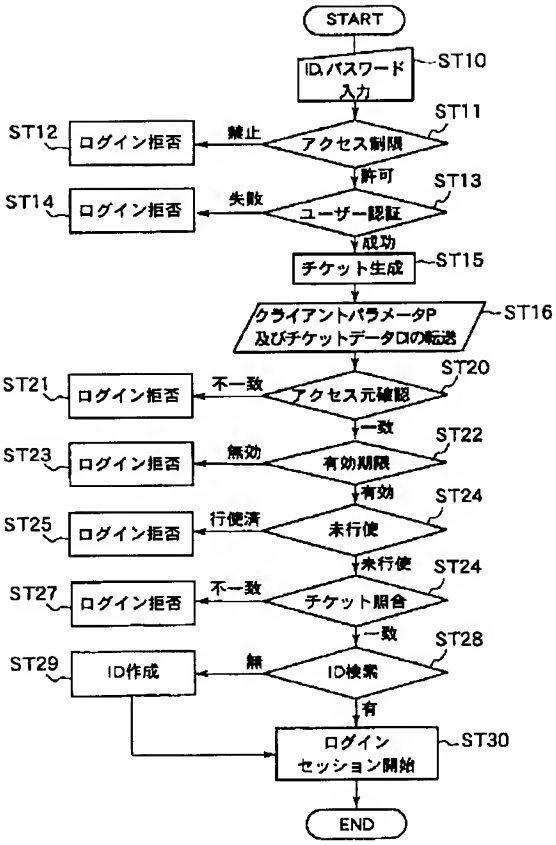
【図１】




【図２】



【図３】


START
ID,パスワード入力
ST10
アクセス制限
ST11
禁止
ST12
ログイン拒否
許可
ユーザー認証
ST13
失敗
ST14
ログイン拒否
成功
チケット生成
ST15
クライアントパラメータP及びチケットデータDの転送
ST16
アクセス元確認
ST20
不一致
ST21
ログイン拒否
一致
有効期限
ST22
無効
ST23
ログイン拒否
有効
未行使
ST24
行使済
ST25
ログイン拒否
未行使
チケット照合
ST24
不一致
ST27
ログイン拒否
一致
ID検索
ST28
無
ST29
ID作成
有
ログインセッション開始
ST30
END